IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

BRANDY SINNETT, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ZEROED-IN TECHNOLOGIES, LLC,

Registered Agent:
Keith A. Goode
780 Elkridge landing Road
Suite 208
Linthicum, Maryland 21090

and

DOLLAR TREE, INC.,

Principal Office Address:
500 Volvo Pkwy
Chesapeake, Virginia 23320

Registered Agent:
Corporation Service Company
100 Shockoe Slip, Floor 2,
Richmond, Virginia 23219

Defendants.

Case No. 1:23-cv-03468

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Brandy Sinnett ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendants Zeroed-In Technologies, LLC ("Zeroed-In") and Dollar Tree, Inc. ("Dollar Tree") (collectively, "Defendants") and alleges as follows based on personal knowledge as to her own acts and on investigation conducted by counsel as to all other allegations:

PARTIES

1. Plaintiff Brandy Sinnett is a citizen and resident of Ohio.

2. Defendant Zeroed-In Technologies, LLC is a Florida limited liability company with its principal place of business in Linthicum, Maryland.

3. Defendant Dollar Tree, Inc. is a Virginia corporation with its principal place of business in Chesapeake, Virginia.

JURISDICTION AND VENUE

4. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are Class members who are diverse from Defendants, and (4) there are more than 100 Class members.

5. This Court has general personal jurisdiction over Defendant Zeroed-In Technologies, LLC because Defendant's principal place of business is in this state.

6. This Court has personal jurisdiction over Defendant Dollar Tree, Inc. because it regularly conducts business in Maryland and has sufficient minimum contacts in Maryland. Further, Plaintiff's claims arise out of Defendant Dollar Tree, Inc.'s contacts with this state, including but not limited to Defendant Dollar Tree, Inc.'s interactions with Defendant Zeroed-In Technologies, LLC.

7. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this district.

FACTUAL ALLEGATIONS

I. Background

8. Zeroed-In is based in Linthicum, Maryland and provides data analytics, management, and software services to businesses across the county.

9. Dollar Tree is based in Chesapeake, Virginia and operates over 16,000 retail discount stores across the county.

10. Dollar Tree's employees, like Plaintiff and Class members, provided certain Personal Identifying Information ("PII" or "Personal Information") to Defendants, which is necessary to obtain employment from Dollar Tree.

11. Dollar Tree utilizes Zeroed-In to manage employee data, including employees' Personal Information.

12. As sophisticated companies with an acute interest in maintaining the confidentiality of the Personal Information entrusted to it, Defendants are well-aware of the numerous data breaches that have occurred throughout the United States and their responsibility for safeguarding Personal Information in their possession.

13. Defendants represent to consumers and the public that they possess robust security features to protect Personal Information and that they take their responsibility to protect Personal Information seriously.

14. Zeroed-In's privacy policy states:

> Zeroed-In Technologies, LLC ("Zeroed-In", "We", "Our", "Us") is committed to protecting the privacy of your information.
>
> . . .
>
> We will not review, share, distribute, or reference any Customer Data except as provided in the applicable Zeroed-In Master Subscription Agreement or as may be required by law. We process

> Customer Data in our Service Platform under the direction of our customers. We have no direct relationship with the individuals whose personal data are contained in the Customer Data.
>
> . . .
>
> We employ robust security measures to protect against the loss, misuse and alternation of the personal information under our control. The Sites employ Secure Socket Layer (SSL) technology using both server authentication and data encryption. The Sites are hosted in a secure server environment that uses firewalls, intrusion detection systems, and other advanced technology to protect against interference or access from outside intruders.
>
> However, no method of transmission over the Internet, or method of electronic storage, is 100% secure. Therefore, we cannot guarantee absolute security. It is your responsibility to ensure you are accessing the Sites and Service Platform using an up-to-date web browser. You are also responsible for maintaining the security and confidentiality of any usernames and passwords associated with the Sites.
>
> Keeping your personal information secure is our first priority. We encourage responsible reporting of any vulnerability that may be found in the Sites or Service Platform. We are committed to working with the security community to verify and respond to any potential vulnerability that is reported to us. To report a potential vulnerability or make an inquiry about security on the Sites or Service Platform, please send an e-mail with details to support@Zeroed-In.com. Please provide full details of the suspected vulnerability so our security team may validate and reproduce the issue.[1]

Dollar Tree's privacy policy states:

> We at Dollar Tree, Inc., Dollar Tree Stores, Inc., Family Dollar Stores, Inc., and their affiliates ("Dollar Tree," "We," "Us," or "Our") care deeply about privacy, security, and online safety.
>
> . . .
>
> We respect the importance of privacy.
>
> . . .

[1] https://www.Zeroed-In.com/privacy-policy/.

Personal Information is maintained on our servers or those of our service providers, and is accessible by authorized employees, representatives, and agents as necessary for the purposes described in this Policy.

We use various reasonable and appropriate safeguards (administrative, organizational, technical, electronic, procedural, and physical) to protect the Personal Information we collect and process. Our security controls are designed to maintain an appropriate level of confidentiality, integrity, and availability of your Personal Information. Nonetheless, no such measure is 100% effective; therefore, we do not guarantee that your Personal Information will be secure from theft, loss, or unauthorized access or use, and we make no representation as to the reasonableness, efficacy, or appropriateness of the measures we use to safeguard such Personal Information, nor that information about you will remain secure in all circumstances. In the event of a security incident of which we are required by law to inform you, we may notify you by email, postal mail, or by telephone, if permitted to do so by law.

Our Site permits you to create an account. When you do, you will be prompted to create a password. For your convenience, our Site includes functionality that allows you to remain logged in so that you do not have to re-enter your password each time you want to access your account. If you choose to remain logged in, you should be aware that anyone with access to your device will be able to access and make changes to your account and may be able to make purchases through your account. For that reason, if you choose to remain logged in, we strongly recommend that you take appropriate steps (such as enabling the "Passcode Lock" security feature on your mobile device) to protect against unauthorized access to and use of your account. You are responsible for maintaining the confidentiality of your password, and you are responsible for any access to or use of your account by someone else who has obtained your password, whether or not such access or use has been authorized by you. You should notify us of any unauthorized use of your password or account as specified in the Contact Us section below.

We encourage you to use caution when using the Internet. If you have reason to believe that your interaction with us is no longer secure, please immediately notify us as specified in the Contact Us section below.[2]

[2] https://www.dollartree.com/privacy-policy.

II. The Data Breach

15. According to Zeroed-In, on August 8, 2023, Zeroed-In learned of suspicious activity on its computer network ("Data Breach").[3]

16. Zeroed-In provided further information via a press release:

> **Nature of the Data**
>
> Event On August 8, 2023, Zeroed-In discovered suspicious activity related to certain network systems. Zeroed-In immediately took steps to secure the systems and launched an investigation into the nature and scope of the activity. Through the investigation, it was determined that an unauthorized actor gained access to certain systems between August 7, 2023 and August 8, 2023. While the investigation was able to determine that these systems were accessed, it was not able to confirm all of the specific files that were accessed or taken by the unauthorized actor. Therefore, Zeroed- In conducted a review of the contents of the systems to determine what information was present at the time of the incident, to whom the information relates, and to which Zeroed-In customers the information belonged. This review was completed on August 31, 2023 and Zeroed-In notified Customer of the event because certain individuals associated with them were identified during the review. The information that was present on the systems at the time of the incident includes names, dates of birth, and/or Social Security number. Zeroed-In coordinated notification with Customer and is providing notice to individuals and regulators, as required, on Customer's behalf.
>
> . . .
>
> **Other Steps Taken and To Be Taken**
>
> Upon discovering the event, Zeroed-In moved quickly to investigate and respond to the incident, assess the security of Zeroed-In systems, and identify potentially affected individuals and Zeroed- In customers. Further, Zeroed-In notified federal law enforcement regarding the event. Zeroed- In is also reviewing existing policies and procedures and implemented additional safeguards. Zeroed-In is also providing complimentary access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose information was potentially affected by this incident.

[3] https://pharmerica.com/data-privacy-incident/.

> Additionally, Zeroed-In is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Zeroed-In is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.[4]

17. The Data Breach compromised individuals' names, dates of birth, and Social Security numbers.[5]

18. The Data Breach affected 1,977,486 individuals, including Plaintiff and Class members, who entrusted their Personal Information to Defendants.[6]

19. Zeroed-In sent a breach notification letter to affected individuals on or around November 2023.[7] Plaintiff received the breach notification letter on December 11, 2023.[8]

20. Defendants did not state why they were unable to prevent the Data Breach or which security feature failed.

21. Defendants did not state why they waited three months after the Data Breach before notifying affected individuals.

22. Defendants failed to prevent the Data Breach because they did not adhere to commonly accepted security standards and failed to detect that their databases were subject to a security breach.

---

[4] https://apps.web.maine.gov/online/aeviewer/ME/40/b3993ddd-2443-4645-ae45-f36dc7686236.shtml.
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] A copy of Plaintiff's breach notification letter is attached as Exhibit 1.

III. Plaintiff's Experience

23. Plaintiff was employed by Family Dollar (owned by Defendant Dollar Tree) from approximately June 2019 – June 2021, and as a condition of her employment, provided Defendant with her Private Information.

24. Plaintiff is very careful about sharing her sensitive Private Information and diligently maintains her Private Information in a safe and secure manner. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

25. As a result of the Data Breach, Plaintiff has and will continue to spend time trying to mitigate the consequences of the Data Breach. This includes time spent verifying the legitimacy of communications related to the Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred.

26. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

27. This time has been lost forever and cannot be recaptured. The harm caused to Plaintiff cannot be undone.

28. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

29. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of cybercriminals.

30. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

31. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' control, is protected, and safeguarded from future breaches.

IV. Injuries to Plaintiff and Class Members

32. As a direct and proximate result of Defendants' actions and omissions in failing to protect Plaintiff and Class members' Personal Information, Plaintiff and Class members have been injured.

33. Plaintiff and Class members have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

34. In addition to the irreparable damage that may result from the theft of Personal Information, identity theft victims must spend numerous hours and their own money repairing the impacts caused by a breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[9]

35. In addition to fraudulent charges and damage to their credit, Plaintiff and Class members may spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to

[9] U.S. Dep't of Justice, *Victims of Identity Theft*, *2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

36. Additionally, Plaintiff and Class members have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their Personal Information is used, the diminution in the value or use of their Personal Information, and the loss of privacy.

V. Securing Personal Information and Preventing Breaches

37. Defendants could have prevented this Data Breach by properly securing and encrypting the Personal Information of Plaintiff and Class members. Alternatively, Defendants could have destroyed the data they no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

38. Defendants' negligence in safeguarding the Personal Information of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

39. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Personal Information of Plaintiff and Class members from being compromised.

40. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[10] The FTC describes "identifying information" as "any name or number that may be used, alone or

[10] 17 C.F.R. § 248.201 (2013).

in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[11]

41. The ramifications of Defendants' failure to keep secure the Personal Information of Plaintiff and Class members are long lasting and severe. Once Personal Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

VI. The Value of Personal Information

42. It is well known that Personal Information, and Social Security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

43. People place a high value not only on their Personal Information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[12]

44. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as

[11] *Id.*

[12] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf.

your DNA to hackers."[13] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."[14]

45. The Personal Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[16] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[17]

46. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your

[13] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.
[14] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.
[15] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[16] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[17] *In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

> name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

47. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

48. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19]

49. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

50. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information,

---

[18] Social Security Admin., *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf.

[19] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

personally identifiable information and Social Security numbers are worth more than 10x on the black market."[20]

51. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

52. The fraudulent activity resulting from the Data Breach may not come to light for years.

53. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

54. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Personal Information of Plaintiff and Class members, including Social Security numbers, and of the foreseeable consequences that would occur if their data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members as a result of a breach.

55. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are

[20] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[21] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

incurring and will continue to incur such damages in addition to any fraudulent use of their Personal Information.

56. Defendants were, or should have been, fully aware of the unique type and the significant volume of data contained in the Personal Information that Defendants stored unencrypted, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

57. The injuries to Plaintiff and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Personal Information of Plaintiff and Class members.

VII. Industry Standards for Data Security

58. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Personal Information of Plaintiff and Class Members and the foreseeable consequences that would occur if Defendants' data security system were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members because of a breach.

59. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on their network, amounting to potentially millions of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

60. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[22]

[22] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

61. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, Marriott, T-Mobile, and Capital One, Defendants are, or reasonably should have been, aware of the importance of safeguarding Personal Information, as well as of the foreseeable consequences of their systems being breached.

62. Therefore, the increase in such attacks, and the attendant risk of future attacks, were widely known to the public and to anyone in Defendants' industry, including Defendants.

63. Security standards commonly accepted among businesses that store Personal Information using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for Personal Information;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

64. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[23] and protection of Personal Information[24] which includes basic security standards applicable to all types of businesses.

[23] *Start with Security: A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[24] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

65. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[25]

67. Because Defendants were entrusted with Personal Information, they had, and have, a duty to keep the Personal Information secure.

68. Plaintiff and Class members reasonably expect that when their Personal Information is provided to a sophisticated business for a specific purpose, that business will safeguard their Personal Information and use it only for that purpose.

69. Nonetheless, Defendants failed to prevent the Data Breach. Had Defendants properly maintained and adequately protected their systems, they could have prevented the Data Breach.

CLASS ALLEGATIONS

70. This action is brought as a class action pursuant to Fed. R. Civ. P. 23.

71. The Class is defined as follows:

> **Nationwide Class:** All persons whose Personal Information was maintained on Defendants' servers that was compromised in the Data Breach.
>
> **Dollar Tree Class:** All persons whose Personal Information was maintained by Dollar Tree that was compromised in the Data Breach.

[25] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

72. The Class excludes the following: Defendants, their affiliates, and their current and former employees, officers and directors, and the Judge assigned to this case.

73. The Class definition may be modified, changed, or expanded based upon discovery and further investigation.

74. *Numerosity*: The Class is so numerous that joinder of all members is impracticable, evidenced by the large number of individuals presently known to have been injured by Defendants' conduct. The Class is ascertainable by records in the possession of Defendants or third parties.

75. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendants owed a duty or duties to Plaintiff and Class members to exercise due care in collecting, storing, safeguarding, and obtaining their Personal Information;

b. Whether Defendants breached that duty or those duties;

c. Whether Defendants failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendants was satisfactory to protect Personal Information as compared to industry standards;

e. Whether Defendants misrepresented or failed to provide adequate information regarding the type of security practices used;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiff and Class members' Personal Information secure and prevent loss or misuse of that Personal Information;

g. Whether Defendants acted negligently in connection with the monitoring and protecting of Plaintiff's and Class members' Personal Information;

h. Whether Defendants' conduct was intentional, willful, or negligent;

i. Whether Plaintiff and Class members suffered damages as a result of Defendants' conduct, omissions, or misrepresentations; and

j. Whether Plaintiff and Class members are entitled to injunctive, declarative, and monetary relief as a result of Defendants' conduct.

76. *Typicality*: Plaintiff's claims are typical of the claims of Class members. Plaintiff and Class members were injured and suffered damages in substantially the same manner, have the same claims against Defendants relating to the same course of conduct, and are entitled to relief under the same legal theories.

77. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the Class and have no interests antagonistic to those of the Class. Plaintiff's counsel are experienced in the prosecution of complex class actions, including actions with issues, claims, and defenses similar to the present case.

78. *Predominance and superiority*: Questions of law or fact common to Class members predominate over any questions affecting individual members. A class action is superior to other available methods for the fair and efficient adjudication of this case because individual joinder of all Class members is impracticable and the amount at issue for each Class member would not justify the cost of litigating individual claims. Should individual Class members be required to bring separate actions, this Court would be confronted with a multiplicity of lawsuits burdening the court system while also creating the risk of inconsistent rulings and contradictory judgments. In contrast to proceeding on a case-by-case basis, in which inconsistent results will magnify the delay and expense to all parties and the court system, this class action presents far fewer management difficulties while providing unitary adjudication, economies of scale and comprehensive supervision by a single court. There are no known difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

79. Accordingly, this class action may be maintained pursuant to Fed. R. Civ. P. 23(b)(3).

80. Defendants have acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

81. Accordingly, this class action may be maintained pursuant to Fed. R. Civ. P. 23(b)(2).

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On Behalf of Plaintiff and All Class Members Against All Defendants)

82. All preceding paragraphs are incorporated herein by reference as though fully set forth herein.

83. Defendants owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted Personal Information, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of their systems. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendants knew that it was more likely than not Plaintiff and Class members would be harmed by such exposure of their Personal Information.

84. Defendants' duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiff and Class members, on the other hand. The special relationship arose because Defendants were entrusted with Plaintiff's and Class members' Personal Information, Defendants accepted and held the Personal Information, and Defendants represented that the Personal Information would be kept

secure pursuant to their data security policies. Defendants alone could have ensured that their data security systems and practices were sufficient to prevent or minimize the data breach.

85. Defendants' duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information. Various FTC publications and data security breach orders further form the basis of Defendants' duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

86. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

87. Defendants breached the aforementioned duties when they failed to use security practices that would protect Plaintiff's and Class members' Personal Information, thus resulting in unauthorized third-party access to the Plaintiff and Class members' Personal Information.

88. Defendants further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit their processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff and Class members' Personal Information within their possession, custody, and control.

89. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff and Class members' Personal Information was disseminated and made available to unauthorized third parties.

90. Defendants admitted that Plaintiff and Class members' Personal Information was wrongfully disclosed as a result of the breach.

91. The breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their Personal Information and the greatly enhanced risk of credit fraud or identity theft.

92. By engaging in the forgoing acts and omissions, Defendants committed the common law tort of negligence. For all the reasons stated above, Defendants' conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the Personal Information; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff and Class members' Personal Information.

93. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class members, their Personal Information would not have been compromised.

94. Neither Plaintiff nor the Class contributed to the breach or subsequent misuse of their Personal Information as described in this Complaint. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class members have been put at an increased risk of credit fraud or identity theft, and Defendants have an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendants are liable to Plaintiff and Class members for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year. Defendants are also liable to Plaintiff and Class members to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their Personal Information, including the amount of time Plaintiff and Class members have spent and will continue to spend as a result of Defendants' negligence. Defendants are also liable to Plaintiff and Class members to the extent their Personal Information

has been diminished in value because Plaintiff and Class members no longer control their Personal Information and to whom it is disseminated.

COUNT II

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and Dollar Tree Class Members Against Defendant Dollar Tree)

95. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

96. Defendant invited Plaintiff and Class members to provide their Personal Information to Defendant. As consideration for the benefits Defendant was to administer, Plaintiff and Class members provided their Personal Information to Defendant. When Plaintiff and Class members provided their Personal Information to Defendant, they entered into implied contracts by which Defendant agreed to protect their Personal Information and only use it solely to administer benefits. As part of the offer, Defendant would safeguard this Personal Information using reasonable or industry-standard means.

97. Accordingly, Plaintiff and Class members accepted Defendant's offer to administer benefits and provided Defendant their Personal Information.

98. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant. However, Defendant breached the implied contracts by failing to safeguard Plaintiff's and the Class's Personal Information.

99. The losses and damages Plaintiff and Class members sustained that are described herein were the direct and proximate result of Defendant's breaches of its implied contracts with them. Additionally, because Plaintiff and Class members continue to be parties to the ongoing administration and distribution of benefits under the contracts, and because damages may not provide a complete remedy for the breaches alleged herein, Plaintiff and Class members are

therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their Personal Information from unlawful exposure.

100. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and Defendant is liable to Plaintiff and Class members for associated damages and specific performance.

COUNT III

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and All Class Members Against Defendant Zeroed-In)

101. Plaintiff and the Class repeat and re-allege each and every allegation as if fully set forth herein.

102. Upon information and belief, Zeroed-In entered into contracts with its customers to provide data analytics, management, and software services; services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

103. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their Private Information that Defendant agreed to receive, store, utilize, and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class members were direct and express beneficiaries of such contracts.

104. Defendant knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class members would be harmed.

105. Defendant breached its contract with customers by, among other things, failing to adequately secure Plaintiff's and Class members' Private Information, and, as a result, Plaintiff and Class members were harmed by Defendant's failure to secure their Private Information.

106. As a direct and proximate result of Defendant's breach, Plaintiff and Class members are at a current and ongoing risk of identity theft, and Plaintiff and Class members sustained incidental and consequential damages including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their Private Information, which remains in Defendant's control, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' Private Information.

107. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

108. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT IV

UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members Against All Defendants)

109. All preceding paragraphs are incorporated herein by reference as though fully set forth herein.

110. Plaintiff and Class members have an interest, both equitable and legal, in their Personal Information that was conferred upon, collected by, and maintained by Defendants and that was ultimately compromised in the Data Breach.

111. Defendants, by way of their acts and omissions, knowingly and deliberately enriched themselves by saving the costs they reasonably should have expended on security measures to secure Plaintiff's and Class members' Personal Information.

112. Defendants also understood and appreciated that the Personal Information pertaining to Plaintiff and Class members was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that Personal Information.

113. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such Personal Information—Defendants instead consciously and opportunistically calculated to increase their own profits at the expense of Plaintiff and Class members. Nevertheless, Defendants continued to obtain the benefits conferred on them by Plaintiff and Class members. The benefits conferred upon, received, and enjoyed by Defendants were not conferred gratuitously, and it would be inequitable and unjust for Defendants to retain these benefits.

114. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result. As a result of Defendants' decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiff's and Class members' Personal Information, Plaintiff and

Class members suffered and continue to suffer considerable injuries in the forms of, *inter alia,* attempted identity theft, time and expenses mitigating harms, diminished value of Personal Information, loss of privacy, and increased risk of harm.

115. Thus, Defendants engaged in opportunistic conduct in spite of their duties to Plaintiff and Class members, wherein they profited from interference with Plaintiff's and Class members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendants to retain the benefits they derived as a consequence of their conduct.

116. Accordingly, Plaintiff and Class members respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically, the amounts that Defendants should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class members' Personal Information, and compensatory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for a judgment as follows:

a. For an order certifying the Class, appointing Plaintiff as Class Representative, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory and punitive and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

JURY DEMAND

Plaintiff demands trial by jury.

Dated: December 21, 2023

Respectfully submitted,

/s/Gary Mason
Gary E. Mason (MD Bar # 15033)
Danielle L. Perry*
MASON LLP
5335 Wisconsin Ave NW, Suite 640
Washington, DC 20015
Phone: (202) 640-1160
gmason@masonllp.com
dperry@masonllp.com

Jeffrey S. Goldenberg *
Todd B. Naylor *
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Phone: (513) 345-8291
Facsimile: (513) 345-8294
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com

Charles E. Schaffer *
Nicholas J. Elia *
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone: (215) 592-1500
cschaffer@lfsblaw.com
nelia@lfsblaw.com

Frank A. Bartela*
Patrick J. Brickman*
Shmuel S. Kleinman*
DWORKEN & BERNSTEIN, CO., L.P.A.
60 South Park Place
Painesville, Ohio 44077
Phone: (440) 352-3391
Facsimile: (440) 352-3469
fbartela@dworkenlaw.com
pbrickman@dworkenlaw.com
skleinman@dworkenlaw.com

Counsel for Plaintiff and Proposed Class

** Pro hac vice forthcoming*